

È vietata la riproduzione anche parziale

In risposta alle policy definite internam
il questionario che trovato nel presente
Le informazioni contenute in questo qu
di garanzia della Business Continuity.

L'analisi di queste informazioni potrebt
attraverso una società di consulenza da

Vi assicuriamo che tutte le informazioni
riservatezza.

FORNITORE

SEDE LEGALE

CONTATTO PRIVACY

CONTATTO DPO (se presente)

CONTATTO DEL RESPONSABILE DEL
TRATTAMENTO

CONTATTO BUSINESS CONTINUITY

| SUB-FORNITORI | |
|---|--|
| SUB FORNITORI (Nome, ragione sociale, sede legale) | ATTIVITA' DELEGATE (indicare le attività delegate al sub-fornitore) |
| Sub- fornitore 1 | |
| Sub-fornitore 2... | |
| | |
| | |
| | |

e di quanto riportato nel presente documen

ANAGRAF

ente per il mantenimento della Cyberse
e documento che abbiamo suddiviso per
questionario verranno utilizzate per svolg

de comportare la necessità di un soprall
a noi incaricata: in questo caso vi contati

i fornite saranno classificate “Confidenz

Compi

| DATI DI CONT | |
|--------------|--|
| Nominativo | |
| | |
| | |
| | |

| |
|--|
| |
| |
| |



| |
|---|
| RIFERIMENTO CONTRATTO / SERVIZIO |
| TRATTAMENTI |
| FINALITA' DEL TRATTAMENTO |
| TIPOLOGIA DATI TRATTATI |
| TIPOLOGIA INTERESSATI |
| TRASFERIMENTO IN PAESI EXTRA UE (in caso affermativo indicare Paese) |

CONDIZIONE DI LEGITTIMITA'
TRASFERIMENTO

ATTIVITA' DELEGATE EXTRA UE

LUOGO DI TRATTAMENTO
*(indicare il luogo dove avviene il
trattamento presso il sub-fornitore)*

mento.

ICA FORNITOR

curity e Data Protection in risposta alle richies
argomento.
ere le adeguate valutazioni in ambito Risk Ana

uogo o di un audit da parte di personale interr
teremo per concordare una data utile.

iali”, in accordo al nostro schema di classifica:

lazione a carico del Fornitore

| ATTO DEL FORNITORE |
|--------------------|
| e-mail |
| |
| |
| |

| |
|--|
| |
| |

| |
|--|
| |
| SI DISPONE DELLA NOMINA A SUB-RESPONSABILE DEL TRATTAMENTO (se sì, fornire evidenza della nomina?) |
| |
| |
| |
| |
| |
| |

E

te normative, vi preghiamo di compilare e restituire
analysis ed i necessari adeguamenti anche in un ottica
no incaricato Cybersecurity e Data Protection o
zione, e che saranno trattate con la massima

| contatto telefonico |
|---------------------|
| |
| |
| |

| |
|--|
| |
| |
| |

| |
|-----------------|
| - Limitazione, |
| - Altro (specif |
| |

| |
|---|
| |
| SI DISPONE DI GARANZIE SUFFICIENTI SULLA SICUREZZA DEL TRATTAMENTO DA PARTE DEL SUB-FORNITORE (certificazioni ISO, codici di condotta, DPIA) |
| |
| |
| |
| |
| |
| |

i Dati Personali necessario per l'erogazione del servizio
ificativi, anagrafici, relativi allo stato civile, professionali o relativi all'istru
ari o reddituali, dati di contatto dei contraenti, beneficiari, soggetti intere
Titolare e dei lavoratori;
allo stato di salute dei contraenti, beneficiari, soggetti interessati dai ser

ri dei contraenti, beneficiari, soggetti interessati dai servizi assicurativi de
alla geolocalizzazione;
razione dei fornitori;
tivi e contributivi dei lavoratori
o

ne
one
ne
one
o o modifica

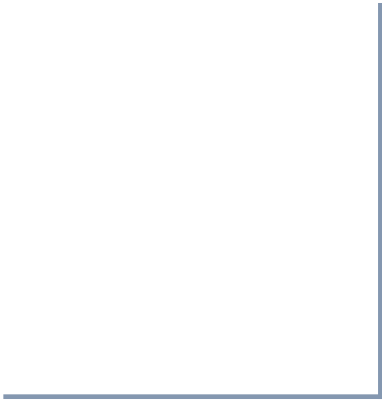
ne

one mediante trasmissione, diffusione o qualsiasi altra forma di messa a d
l'interconnessione

.....
, cancellazione o distruzione
ficare)

uzione,
essati dai servizi
vizi assicurativi del
il Titolare;

isposizione



Adeguamento al GD

Requisiti Richiesti

Requisiti generali dei fornitori (Sub-Responsabili del trattamento)

| | |
|----------|--|
| 1 | La Società ha qualche certificazione in ambito privacy? Se sì indicare quali |
| 2 | La Società ha aderito a codici di Condotta di Associazioni di Categoria? |
| 3 | La Società ha proceduto alla nomina di un DPO (Data Protection Officer)? |
| 4 | La Società ha individuato una funzione interna deputata alla gestione degli adempimenti privacy? |
| 5 | La Società ha adottato un Registro dei trattamenti, un "Documento Programmatico per la protezione dei Dati Personali" o un qualche documento analogo? Se sì, indicare se tale documento è oggetto di aggiornamenti periodici (colonna E) |
| 6 | La società ha adottato PROCEDURE E POLICY PRIVACY ? Se sì indicare quali |
| 7 | La Società procede ad un'attività di formazione verso ciascun dipendente/collaboratore? Se sì indicare periodicità e modalità erogazione formazione |
| 8 | La Società procede ad un aggiornamento periodico delle nomine ad incaricati / responsabili / amministratori di sistema? |

| | |
|-----------|--|
| 9 | Gli Amministratori di Sistema sono stati nominati internamente o esternamente? |
| 10 | Gli ADS sono stati nominati tali tramite documento formale? |
| 11 | Designazioni individuali: è stata fatta la designazione individuale quale amministratore di sistema che reca l'elencazione analitica degli ambiti di operatività (job description) consentiti in base al profilo di autorizzazione assegnato? |
| 12 | È adottato un idoneo sistema per la registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici? (Se SI specificare come) |
| 13 | Tali registrazioni (access log) hanno caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste? |
| 14 | Le registrazioni (access log) comprendono i riferimenti temporali e la descrizione dell'evento che le ha generate e sono conservate per un congruo periodo, non inferiore a sei mesi? |
| 15 | È utilizzata la cifratura dei log? In caso negativo, sono presenti altri sistemi di protezione dei log? |
| 16 | I registri (access log) sono conservati in un repository protetto o non accessibile da parte dell'AdS? |
| 17 | Viene effettuata con cadenza almeno annuale una verifica sull'operato degli amministratori di sistema in modo da controllare la rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati personali? |
| 18 | La Società ha adottato un sistema operativo per la gestione delle politiche e delle procedure per la sicurezza delle informazioni? |
| 19 | Esiste un indirizzo e-mail o call center dedicato per la notifica delle violazioni di dati personali? |
| 20 | Prima di procedere alla nomina di eventuali Sub-Responsabili, è stata richiesta l'autorizzazione scritta al Titolare? |
| 21 | È stata verificata (ed è verificata almeno con cadenza annuale) l'adeguatezza delle misure tecniche e organizzative di ogni eventuale Sub-Responsabile tramite la compilazione della presente Checklist di Conformità al momento dell'attribuzione dell'incarico, e con cadenza annuale? |

| | |
|-----------|--|
| 22 | Gli eventuali Sub-Responsabili del trattamento sono stati nominati tali sulla base di un accordo i cui contenuti sono sostanzialmente analoghi al presente Atto? |
| 23 | Il fornitore è stato mai oggetto di un'ispezione del Garante della Privacy? <u>[se sì, specificare l'oggetto dell'Ispezione]</u> |
| 24 | Il Partner ha mai subito e comunicato un data Breach? <u>[se sì indicare l'oggetto del data breach]</u> |

Copyright © 2022 – Nethive SPA
È vietata la riproduzione anche parziale di quanto pubblicato senza permesso scritto dalla Nethive SPA.
Il presente materiale è consegnato come base di partenza per la compilazione e deve essere adeguato ai contenuti e alla propria struttura e alle procedure della propria azienda.

PR - Misure Organizzative

| Campi per il Fornitore | |
|---|---|
| Valutazione stato di applicazione del requisito | Integrazione requisito ed evidenze a supporto |
| 2 | |
| 2 | |
| 2 | |
| 2 | |
| 2 | |
| | |
| | |
| | |

[illegible]

| | |
|--|--|
| | |
| | |
| | |

24

48

0

48

10

0,2083333333333333

a la preventiva autorizzazione scritta di Nethive.
ostruzione di un proprio impianto o sistema di gestione. Si consiglia di
azienda.

| LEGENDA STATO IMPLEMENTAZIONE | |
|-------------------------------|---------------------------------------|
| 0 | Non ancora implementato/pianificato |
| 1 | Parzialmente implementato/Pianificato |
| 2 | Completamente implementato |
| N/A | Non Applicabile |

(es: certificazione ISO 27001 del 2013)
Si prega di allegare copia della certificazione

Tali codici forniscono orientamenti dettagliati che adattano i requisiti di legge a settori specifici e promuovono la trasparenza delle attività di trattamento.

Le società possono utilizzare l'adesione ai codici come prova a dimostrazione della loro conformità con il diritto dell'UE e come mezzo per rafforzare la loro immagine pubblica in quanto organizzazioni che attribuiscono la priorità alla protezione dei dati e si impegnano in tal senso nello svolgimento delle loro attività.

| |
|---|
| <p>La designazione di tale figura rimane una pratica fortemente raccomandata, in ossequio al principio di accountability che permea l'intero GDPR, e che sarà positivamente considerata, quale misura di responsabilizzazione.</p> |
| <p>Ad es. Ufficio Privacy; Ufficio Legale; Ufficio compliance</p> |
| <p>La tenuta del registro dei trattamenti è prevista dall'articolo 30 del GDPR, ed è considerata indice di una corretta gestione dei trattamenti. Si prega di allegare l'estratto del Registro del responsabile tenuto per conto del Cliente</p> |
| <p>Si tratta di documenti finalizzati a disciplinare la corretta implementazione della normativa privacy. (es: Procedura di data breach, Procedura gestione riscontro richieste interessati) Si prega di allegare le procedure adottate in ambito privacy compresa quella indicata.</p> |
| <p>La formazione aziendale in ambito privacy è necessaria per rendere i soggetti autorizzati al trattamento dei dati consapevoli dei trattamenti di dati personali che svolgono quotidianamente, ma anche per limitare i rischi relativi alla sicurezza ed evitare di incorrere perciò in eventuali sanzioni.</p> |
| <p>I documenti di autorizzazione/designazione al trattamento dei dati sono importanti per definire l'organigramma privacy oltre che per stabilire ed impartire le istruzioni cui tali soggetti sono tenuti ad attenersi.</p> |
| <p>Si prega di allegare il documento</p> |

Ad es. Sistema di gestione della sicurezza delle informazioni (ISMS).

Politica

rischio, ambientali) sono compresi e uti

Requisiti Richiesti

Requisiti generali dei fornitori

| | |
|----------|---|
| 1 | È indentificata e resa nota una policy di cybersecurity |
| 2 | Ruoli e responsabilità inerenti la cybersecurity sono coordinati ed allineati con i ruoli interni ed i partner esterni |
| 3 | I requisiti legali in materia di cybersecurity, con l'inclusione degli obblighi riguardanti la privacy e le libertà civili, sono compresi e gestiti |
| 4 | La governance ed i processi di risk management includono la gestione dei rischi legati alla cybersecurity |

Copyright © 2022 – Nethive SPA

È vietata la riproduzione anche parziale di quanto pubblicato senza permesso scritto dalla Nethive SPA.
Il presente materiale è consegnato come base di partenza per la compilazione del questionario. La Nethive SPA consiglia di adeguare i contenuti e alla propria struttura e alle procedure.

Cybersecurity

Utilizzati nella gestione del rischio di cybersecurity.

Campi per il Fornitore

| Valutazione stato di applicazione del requisito | Integrazione requisito ed evidenze a supporto |
|---|---|
| 2 | |
| 1 | |
| 0 | |
| 2 | |

ADEGUATO

VALUTAZIONE IMPLEMENTAZIONE REQUISITI

a la preventiva autorizzazione scritta di Nethive.
ostruzione di un proprio impianto o sistema di gestione. Si
edure della azienda.

| LEGENDA STATO IMPLEMENTAZIONE | |
|-------------------------------|---------------------------------------|
| 0 | Non ancora implementato/pianificato |
| 1 | Parzialmente implementato/Pianificato |
| 2 | Completamente implementato |
| N/A | Non Applicabile |

| | |
|----------|------------------------------|
| 1 | Risk Assessment |
| 2 | Risk Analysis |
| 2 | Risk Treatment |
| 3 | Acceptance risk management |
| 4 | Supply Chain Risk Management |
| 5 | Supply Chain Risk Management |

Copyright © 2022 – Nethive SPA

È vietata la riproduzione anche parziale di quanto pubblicato.
Il presente materiale è consegnato come base di partenza
propria struttura e alle procedure della azienda.

Risk M

le funzioni, l'immagine o la r

Le priorità e i requisiti dell'organizzazione e la tol

Requisiti Richiesti

Requisiti generali dei fornitori

E' stata sviluppata una strategia globale per la gestione dei rischi, nell'ambito della quale sono inclusi/previsti i rischi associati al sistema informativo

Periodicamente è revisionata e aggiornata la strategia di gestione dei rischi e, se necessario, si interviene su di essa per renderla coerente con eventuali variazioni di contesto (es. cambiamenti organizzativi, introduzione di nuovi processi, adozione di nuove tecnologie, ecc.).

L'organizzazione formula un piano di trattamento del rischio tenendo conto dei risultati della valutazione del rischio che insiste sul sistema informativo, in coerenza con il livello di rischio accettabile (risk appetite) e i livelli di tolleranza stabiliti dall'organizzazione stessa (risk tolerance).

Il piano di trattamento considera tutti i controlli necessari per assicurare un livello di sicurezza della rete e dei sistemi informativi adeguato al rischio esistente.

Eventuali rischi accettati sono adeguatamente documentati.

Nell'ambito della strategia di gestione dei rischi e nel contesto della formulazione del piano di trattamento vengono presi in esame i rischi legati ai fornitori esterni e terze parti, con particolare riferimento alle catene di fornitura legate all'erogazione dei servizi essenziali.

Fornitori e partner terzi sono regolarmente valutati utilizzando audit, verifiche, o altre forme di valutazione per confermare il rispetto degli obblighi contrattuali

ato senza la preventiva autorizzazione scritta di Nethive.
e per la costruzione di un proprio impianto o sistema di gestione. Si

Management

eranza al rischio sono definiti e utilizzati per supportare

| Campi per il Fornitore | |
|------------------------|--|
|------------------------|--|

| Valutazione stato di | |
|----------------------|--|
| | |

| applicazione del requisito | Integrazione requisito ed evidenze a supporto |
|----------------------------|---|
|----------------------------|---|

| | |
|--|--|
| | |
| | |
| | |
| | |
| | |
| | |

o

VALUTAZIONE IMPLEMENTAZIONE REQUISITI

consiglia di adeguare i contenuti e alla

| LEGENDA STATO IMPLEMENTAZIONE | |
|-------------------------------|---------------------------------------|
| 0 | Non ancora implementato/pianificato |
| 1 | Parzialmente implementato/Pianificato |
| 2 | Completamente implementato |
| N/A | Non Applicabile |

Adeguamento al

Requisiti Richiesti

Requisiti generali dei fornitori

| | |
|-----------|--|
| 1 | Esistono misure tecniche in grado di tracciare i dati personali nei sistemi informatici? |
| 2 | Se presenti, le particolari categorie di dati personali hanno un accesso separato dagli altri dati personali? Se sì, quale? |
| 3 | Esistono misure tecniche in grado di tracciare i dati personali in formato cartaceo? |
| 4 | Se presenti, le particolari categorie di dati personali hanno un accesso separato dagli altri dati personali? Se sì, quale? |
| 5 | Esistono delle misure tecniche volte ad identificare e/o prevenire eventuali trattamenti dei dati personali secondo finalità diverse da quelle previste dall'Atto? |
| 6 | Esistono delle misure tecniche in grado di consentire la cancellazione, la modifica, l'aggiornamento, la limitazione del trattamento e la portabilità dei dati personali a richiesta del Titolare e/o alla cessazione dell'Atto? |
| 7 | Esistono delle misure tecniche che consentono la restituzione dei dati personali al Titolare, a richiesta della stessa e/o alla cessazione dell'Atto? |
| 8 | Gli accessi degli incaricati ai sistemi informatici sono protetti tramite codice-id e password? |
| 9 | La password di accesso ai sistemi informatici utilizzata da ogni Persona Autorizzata è di almeno 14 caratteri, non facilmente riconducibile all'incaricato (quindi non uguale alla log-in) e modificata al primo utilizzo e ogni 3 mesi? |
| 10 | Vengono utilizzati unicamente account personali e nominali per poter accedere ai dati personali? |

Copyright © 2022 – Nethive SPA

È vietata la riproduzione anche parziale di quanto pubblicato senza permesso scritto dalla casa editrice. Il presente materiale è consegnato come base di partenza per la costruzione di nuovi percorsi didattici. Si consiglia di adeguare i contenuti e alla propria struttura e alle proprie esigenze.

GDPR - Misure Tecniche

Campi per il Fornitore

[illegible]

o

VALUTAZIONE IMPLEMENTAZIONE REQUISITI

a la preventiva autorizzazione scritta di Nethive.
ostruzione di un proprio impianto o sistema di gestione. Si
edure della azienda.

| LEGENDA STATO IMPLEMENTAZIONE | |
|-------------------------------|---------------------------------------|
| 0 | Non ancora implementato/pianificato |
| 1 | Parzialmente implementato/Pianificato |
| 2 | Completamente implementato |
| N/A | Non Applicabile |

Obie

| | |
|----------|--|
| 1 | Perimetro di sicurezza |
| 2 | Controlli di accesso fisico |
| 3 | Rendere sicuri uffici, locali e strutture |
| 4 | Protezione contro le minacce esterne ed ambientali |
| 5 | Aree di carico e scarico |

| | |
|----------|--|
| 6 | Apparecchiature incustodite degli utenti |
| 7 | Politica schermo e scrivania puliti |

| | |
|-----------|--|
| 8 | Politica controllo degli accessi logici |
| 9 | Accesso alle reti e ai servizi di rete |
| 10 | Provisioning degli accessi utenti |
| 11 | Gestione dei diritti di accesso privilegiato |
| 12 | Gestione delle informazioni segrete di autenticazione degli utenti |
| 13 | Riesame dei diritti di accesso degli utenti |
| 14 | Rimozione o adattamento dei diritti di accesso |
| 15 | Limitazione dell'accesso alle informazioni |
| 16 | Procedure di log-on sicure |
| 17 | Sistema di gestione delle password |
| 18 | Uso di programmi di utilità privilegiati |
| 19 | Controllo degli accessi al codice sorgente dei programmi |
| 20 | Controlli di rete |

| | |
|-----------|-------------------------------|
| 21 | Sicurezza dei servizi di rete |
| 22 | Segregazione delle reti |

Copyright © 2022 – Nethive SPA

È vietata la riproduzione anche parziale di quanto pubblicato.
Il presente materiale è consegnato come base di partenza per la propria struttura e alle procedure della azienda.

Contro

Requisiti Richiesti

Requisiti generali dei fornitori

Controllo di accesso fisico agli uffici

Obiettivo: Nessun accesso fisico non autorizzato ai

Sono definiti perimetri di sicurezza per proteggere le aree che contengono informazioni critiche e le strutture di elaborazione delle informazioni.

Le aree di sicurezza devono essere protette da appropriati controlli per l'ingresso atti ad assicurare che solo il personale autorizzato abbia il permesso di accedervi.

Deve essere progettata e applicata la sicurezza fisica agli uffici, ai locali ed agli impianti.

Deve essere progettata e applicata un'adeguata protezione fisica da calamità naturali, attacchi malevoli e accidentali.

I punti di accesso, come le aree di carico e scarico e altri punti attraverso i quali persone non autorizzate potrebbero accedere ai locali, devono essere controllati e, se possibile, isolati dalle strutture di elaborazione delle informazioni per evitare accessi non autorizzati.

Controllo di accesso logico ai

Obiettivo: Nessun accesso non autorizzato ai

Gli utenti devono assicurare che i device/sistemi, se incustoditi, siano appropriatamente protetti.

Adozione di una politica di CLEAR DESK POLICY e CLEAR SCREEN POLICY.

Adozione di una politica di controllo degli accessi logici aggiornata sulla base dei requisiti di business e di sicurezza delle informazioni

Agli utenti devono essere forniti solo gli accessi alle reti ed ai servizi di rete per il cui uso sono stati specificamente autorizzati.

Deve essere attuato un processo formale per l'assegnazione o la revoca dei diritti di accesso per tutte le tipologie di utenze e per tutti i sistemi e servizi.

L'assegnazione e l'uso di diritti di accesso privilegiato devono essere limitati e controllati.

L'assegnazione delle informazioni segrete di autenticazione deve essere controllata attraverso un processo di gestione formale e gli utenti devono essere tenuti a seguire la prassi dell'organizzazione nell'uso di informazioni segrete di autenticazione.

I responsabili degli asset devono riesaminare ad intervalli regolari i diritti di accesso degli utenti.

I diritti di accesso di tutto il personale e degli utenti di parti esterne a informazioni e strutture di elaborazione delle informazioni devono essere rimossi al momento della cessazione del rapporto di lavoro, del contratto o accordo, oppure adattate a ogni variazione.

L'accesso a informazioni e funzioni di sistemi applicativi deve essere limitato.

Quando richieste dalle politiche di controllo degli accessi, l'accesso a sistemi e applicazioni deve essere controllato da procedure di log-on sicure (Strong Authentication).

I sistemi di gestione delle password devono essere interattivi e devono assicurare password di con criteri di complessità definiti dall'organizzazione.

L'uso di programmi di utilità che potrebbero essere in grado di aggirare i controlli applicativi e di sistema deve essere limitato e strettamente controllato.

Gli accessi al codice sorgente dei programmi devono essere limitati al solo personale autorizzato.

Le reti devono essere gestite e controllate per proteggere le informazioni nei sistemi e nelle applicazioni.

I meccanismi di sicurezza, i livelli di servizio e i requisiti di gestione di tutti i servizi di rete devono essere identificati e inclusi negli accordi sui livelli di servizio relativi alla rete, indipendentemente dal fatto che tali servizi siano forniti dall'interno o dall'esterno.

Nelle reti si devono segregare gruppi di servizi, di utenti e di sistemi informativi sulla base del loro livello di criticità per permettere l'adozione di misure di sicurezza proporzionate al rischio.

ato senza la preventiva autorizzazione scritta di Nethive.
e per la costruzione di un proprio impianto o sistema di gestione. Si

llo di accessi

| Campi per il Fornitore | |
|---|---|
| Valutazione stato di applicazione del requisito | Integrazione requisito ed evidenze a supporto |

fici e al Sistema di elaborazione dei dati

i sistemi di elaborazione dati.

| | |
|--|--|
| | |
| | |
| | |
| | |
| | |

al sistema di elaborazione dei dati

sistemi di informazione

| | |
|--|--|
| | |
| | |

[illegible]

| | |
|--|--|
| | |
| | |

| | |
|---|---------------------------------------|
| o | VALUTAZIONE IMPLEMENTAZIONE REQUISITI |
|---|---------------------------------------|

consiglia di adeguare i contenuti e alla

| LEGENDA STATO IMPLEMENTAZIONE | |
|-------------------------------|---------------------------------------|
| 0 | Non ancora implementato/pianificato |
| 1 | Parzialmente implementato/Pianificato |
| 2 | Completamente implementato |
| N/A | Non Applicabile |

Obiettivo: Nessuna op

| | |
|----------|---|
| 1 | Politiche e procedure per il trasferimento delle informazioni |
| 2 | Accordi di trasferimento delle informazioni |
| 3 | Messaggistica elettronica |
| 4 | Accordi di riservatezza o di non divulgazione |
| 5 | Utilizzo di controlli crittografici |

Copyright © 2022 – Nethive SPA

È vietata la riproduzione anche parziale di quanto pubblicato.
Il presente materiale è consegnato come base di partenza per la propria struttura e alle procedure della azienda.

Controllo d

Requisiti Richiesti

Requisiti generali dei fornitori (Sub-Responsabili del trattamento)

Operazione di lettura, copia, modifica o cancellazione e trasporto elettronico

Devono esistere politiche, procedure e controlli a protezione del trasferimento delle informazioni.

I trasferimenti sicuri di informazioni di business tra l'organizzazione e le parti esterne devono essere indirizzati in appositi accordi.

Le informazioni trasmesse attraverso messaggistica elettronica devono essere protette in modo appropriato.

I requisiti per gli accordi di riservatezza o di non divulgazione che riflettono le necessità dell'organizzazione per la protezione delle informazioni devono essere identificati, riesaminati periodicamente e documentati.

Devono essere utilizzati controlli crittografici per la protezione delle informazioni critiche. Le chiavi crittografiche sono protette per il loro intero ciclo di vita.

ato senza la preventiva autorizzazione scritta di Nethive.
e per la costruzione di un proprio impianto o sistema di gestione. Si

el trasferimento

| Campi per il Fornitore | |
|---|---|
| Valutazione stato di applicazione del requisito | Integrazione requisito ed evidenze a supporto |

zione non autorizzata durante la trasmissione o il

| | |
|--|--|
| | |
| | |
| | |
| | |
| | |

consiglia di adeguare i contenuti e alla

| LEGENDA STATO IMPLEMENTAZIONE | |
|-------------------------------|---------------------------------------|
| 0 | Non ancora implementato/pianificato |
| 1 | Parzialmente implementato/Pianificato |
| 2 | Completamente implementato |
| N/A | Non Applicabile |

| | |
|----------|--------------------------------------|
| 1 | Raccolta di log degli eventi |
| 2 | Protezione delle informazioni di log |
| 3 | Log di amministratori e operatori |
| 4 | Sincronizzazione degli orologi |
| 5 | Utilizzo di controlli crittografici |

Copyright © 2022 – Nethive SPA

È vietata la riproduzione anche parziale di quanto pubblicato.
Il presente materiale è consegnato come base di partenza propria struttura e alle procedure della azienda.

Controllo

Obiettivo: Tracciatura di inserimenti, modifiche

Requisiti Richiesti

Requisiti generali dei fornitori

La registrazione dei log degli eventi, delle attività degli utenti, delle eccezioni, dei malfunzionamenti e degli eventi relativi alla sicurezza delle informazioni deve essere effettuata, mantenuta e riesaminata periodicamente.

Le strutture per la raccolta del log e le informazioni di log devono essere protette da manomissioni e accessi non autorizzati.

Le attività degli amministratori e degli operatori di sistema devono essere sottoposte a log, e questi devono essere protetti e riesaminati periodicamente.

Gli orologi di tutti i sistemi pertinenti che elaborano informazioni all'interno di un'organizzazione o di un dominio di sicurezza devono essere sincronizzati rispetto a una singola sorgente temporale di riferimento.

Devono essere utilizzati controlli crittografici per la protezione delle informazioni critiche. Le chiavi crittografiche sono protette per il loro intero ciclo di vita.

ato senza la preventiva autorizzazione scritta di Nethive.
e per la costruzione di un proprio impianto o sistema di gestione. Si

delle modifiche
ifiche o cancellazione di dati dai sistemi informativi.

| Campi per il Fornitore | |
|---|---|
| Valutazione stato di applicazione del requisito | Integrazione requisito ed evidenze a supporto |

| | |
|--|--|
| | |
| | |
| | |
| | |
| | |

consiglia di adeguare i contenuti e alla

| LEGENDA STATO IMPLEMENTAZIONE | |
|-------------------------------|---------------------------------------|
| 0 | Non ancora implementato/pianificato |
| 1 | Parzialmente implementato/Pianificato |
| 2 | Completamente implementato |
| N/A | Non Applicabile |

| | |
|----------|--|
| 1 | Disposizione delle apparecchiature e loro protezione |
| 2 | Infrastruttura di supporto |
| 3 | Sicurezza dei cablaggi |
| 4 | Manutenzione delle apparecchiature |
| 5 | Procedure operative |
| 6 | Gestione dei cambiamenti |
| 7 | Controlli contro malware |

| | |
|-----------|--|
| 8 | Installazione del software sui sistemi di produzione |
| 9 | Gestione delle vulnerabilità tecniche |
| 10 | Limitazioni all'installazione del software |
| 11 | Controlli per l'audit sui sistemi informativi |

Copyright © 2022 – Nethive SPA

È vietata la riproduzione anche parziale di quanto pubblicato.
Il presente materiale è consegnato come base di partenza propria struttura e alle procedure della azienda.

Controllo della

Obiettivo: Protezione contro perd

Requisiti Richiesti

Requisiti generali dei fornitori

Le apparecchiature devono essere disposte e protette al fine di ridurre i rischi derivanti dalle minacce e dai pericoli ambientali, oltre alle occasioni di accesso non autorizzato.

Le apparecchiature devono essere protette da malfunzionamenti alla rete elettrica di alimentazione e da altri disservizi causali da malfunzionamenti dei servizi ausiliari.

I cavi per l'energia elettrica e le telecomunicazioni adibiti al trasporto di dati o a supporto di servizi informatici devono essere protetti da intercettazioni, interferenze o danneggiamenti.

Le apparecchiature devono essere correttamente mantenute per assicurare la loro continua disponibilità e integrità.

Devono essere documentate e rese disponibili delle procedure operative a tutti gli utenti che le necessitano.

I cambiamenti all'organizzazione, ai processi di business, alle infrastrutture di elaborazione delle informazioni e ai sistemi che potrebbero influenzare la sicurezza delle informazioni devono essere controllati.

Devono essere attuati controlli di individuazione, di prevenzione e di ripristino relativamente al malware, congiuntamente ad un'appropriata consapevolezza degli utenti.

Devono essere attuate procedure per controllare l'installazione del software sui sistemi di produzione.

Le informazioni sulla vulnerabilità tecniche dei sistemi informativi utilizzati devono essere ottenute in modo tempestivo, l'esposizione a tali vulnerabilità deve essere valutata e appropriate misure devono essere intraprese per affrontare i rischi relativi.

Devono essere stabilite e attuate regole per il governo dell'installazione del software da parte degli utenti.

I requisiti e le attività di audit che prevedono una verifica dei sistemi di produzione devono essere attentamente pianificati e concordati per minimizzare le interferenze con i processi di business

disponibilità dei dati

Perdite o distruzioni accidentali o intenzionali

Campi per il Fornitore

Valutazione stato di applicazione del requisito

Integrazione requisito ed evidenze a supporto

[illegible]

| | |
|--|--|
| | |
| | |
| | |
| | |

| | |
|---|---------------------------------------|
| o | VALUTAZIONE IMPLEMENTAZIONE REQUISITI |
|---|---------------------------------------|

consiglia di adeguare i contenuti e alla

| LEGENDA STATO IMPLEMENTAZIONE | |
|-------------------------------|---------------------------------------|
| 0 | Non ancora implementato/pianificato |
| 1 | Parzialmente implementato/Pianificato |
| 2 | Completamente implementato |
| N/A | Non Applicabile |

| | |
|----------|---|
| 1 | Backup delle informazioni |
| 2 | Pianificazione della continuità della sicurezza delle informazioni |
| 3 | Attuazione della continuità della sicurezza delle informazioni |
| 4 | Verifica, riesame e valutazione della continuità della sicurezza delle informazioni |
| 5 | Disponibilità delle strutture per l'elaborazione delle informazioni |

Copyright © 2022 – Nethive SPA

È vietata la riproduzione anche parziale di quanto pubblicato.
Il presente materiale è consegnato come base di partenza per la propria struttura e alle procedure della azienda.

Capacità di recupero (R)

Obiettivo: Capacità di recupero entro un periodo

Requisiti Richiesti

Requisiti generali dei fornitori

Devono essere effettuate copie di backup delle informazioni, dei software e delle immagini dei sistemi e quindi sottoposte a test periodici secondo una politica di backup concordata.

L'organizzazione deve determinare i propri requisiti per la sicurezza delle informazioni e per la continuità della gestione della sicurezza delle informazioni in situazioni avverse, per esempio durante crisi o disastri.

L'organizzazione deve stabilire, documentare, attuare e mantenere processi, procedure e controlli per assicurare il livello di continuità richiesto per la sicurezza delle informazioni durante una situazione avversa.

L'organizzazione deve verificare ad intervalli di tempo regolari i controlli di continuità della sicurezza delle informazioni stabiliti e attuati, al fine di assicurare che siano validi ed efficaci durante situazioni avverse.

Le strutture per l'elaborazione delle informazioni devono essere realizzate con una ridondanza sufficiente a soddisfare i requisiti di disponibilità.

ato senza la preventiva autorizzazione scritta di Nethive.
e per la costruzione di un proprio impianto o sistema di gestione. Si

Art. 32 Sezione 1 lit. c GDPR)

periodo di tempo appropriato dopo un evento di
disturbo.

| Campi per il Fornitore | |
|---|---|
| Valutazione stato di applicazione del requisito | Integrazione requisito ed evidenze a supporto |

| | |
|--|--|
| | |
| | |
| | |
| | |
| | |

consiglia di adeguare i contenuti e alla

| LEGENDA STATO IMPLEMENTAZIONE | |
|-------------------------------|---------------------------------------|
| 0 | Non ancora implementato/pianificato |
| 1 | Parzialmente implementato/Pianificato |
| 2 | Completamente implementato |
| N/A | Non Applicabile |

| | |
|----------|---|
| 1 | Responsabilità e procedure |
| 2 | Segnalazione degli eventi relativi alla sicurezza delle informazioni |
| 3 | Data Breach |
| 4 | Valutazione e decisione sugli eventi relativi alla sicurezza delle informazioni |
| 5 | Risposta agli incidenti relativi alla sicurezza delle informazioni |
| 6 | Raccolta evidenze |

Copyright © 2022 – Nethive SPA

È vietata la riproduzione anche parziale di quanto pubblicato.
Il presente materiale è consegnato come base di partenza per la propria struttura e alle procedure della azienda.

Incidenti

Obiettivo: Capacità di gestire gli incidenti

Requisiti Richiesti

Requisiti generali dei fornitori

Devono essere stabilite le responsabilità e le procedure di gestione degli incidenti per assicurare una risposta rapida, efficace ed ordinata agli incidenti relativi alla sicurezza delle informazioni.

Gli eventi relativi alla sicurezza delle informazioni devono essere segnalati il più velocemente possibile attraverso appropriati canali gestionali.

E' presente una procedura per l'individuazione e la gestione dei Data Breach, che comprende la notifica al Garante e agli Interessati.

Gli eventi relativi alla sicurezza devono essere valutati e deve essere deciso se classificarli come incidenti relativi alla sicurezza delle informazioni.

Si deve rispondere agli incidenti relativi alla sicurezza delle informazioni in accordo alle procedure documentate.

L'organizzazione deve definire ed applicare opportune procedure per l'identificazione, la raccolta, l'acquisizione e la conservazione delle informazioni che possono essere impiegate come evidenze

ato senza la preventiva autorizzazione scritta di Nethive.
e per la costruzione di un proprio impianto o sistema di gestione. Si

Management

cidenti efficacemente ed efficientemente

| Campi per il Fornitore | |
|---|---|
| Valutazione stato di applicazione del requisito | Integrazione requisito ed evidenze a supporto |

| | |
|--|--|
| | |
| | |
| | |
| | |
| | |
| | |

consiglia di adeguare i contenuti e alla

| LEGENDA STATO IMPLEMENTAZIONE | |
|-------------------------------|---------------------------------------|
| 0 | Non ancora implementato/pianificato |
| 1 | Parzialmente implementato/Pianificato |
| 2 | Completamente implementato |
| N/A | Non Applicabile |

| | |
|----------|------------------------------|
| 1 | Eventi e Anomalie |
| 2 | Monitoraggio della Security |
| 3 | Gestione delle Vulnerabilità |
| 5 | Audit |
| 6 | KPI |

Copyright © 2022 – Nethive SPA

È vietata la riproduzione anche parziale di quanto pubblicato.
Il presente materiale è consegnato come base di partenza propria struttura e alle procedure della azienda.

Mor

Requisiti Richiesti

Requisiti generali dei fornitori

Sono adottate misure e tecniche permettono di identificare le attività anomale e il loro impatto potenziale viene analizzato.
Gli eventi rilevati vengono analizzati per comprendere gli obiettivi e le metodologie dell'attacco.
Le informazioni relative agli eventi sono raccolte e correlate da sensori e sorgenti multiple.

I sistemi informativi e gli asset sono monitorati per indentificare eventi di cybersecurity e per verificare l'efficacia delle misure di protezione.
Viene svolto il monitoraggio della rete informatica per rilevare potenziali eventi di cybersecurity.

E' presente un processo di individuazione delle vulnerabilità (patch, aggiornamenti di security) su tutti gli asset presenti in rete.
Vengono svolte scansioni per l'identificazione di vulnerabilità.
Le Vulnerabilità individuate sono analizzate e sono adottare idonee misure affinché queste possano essere gestite.
Le nuove vulnerabilità sono mitigate o documentate come rischio accettato

Sono organizzati e svolti periodici audit con l'obiettivo di monitorare la corretta esecuzione delle attività pianificate.
Gli audit sono documentanti.

Sono definiti KPO e calcolati i relativi KPI per verificare il soddisfacimento di obiettivi e performance relativi alle attività di security e per il soddisfacimento dei requisiti contrattualizzati

ato senza la preventiva autorizzazione scritta di Nethive.
e per la costruzione di un proprio impianto o sistema di gestione. Si

Monitoraggio

| Campi per il Fornitore | |
|---|---|
| Valutazione stato di applicazione del requisito | Integrazione requisito ed evidenze a supporto |

| | |
|--|--|
| | |
| | |
| | |
| | |
| | |

consiglia di adeguare i contenuti e alla

| LEGENDA STATO IMPLEMENTAZIONE | |
|-------------------------------|---------------------------------------|
| 0 | Non ancora implementato/pianificato |
| 1 | Parzialmente implementato/Pianificato |
| 2 | Completamente implementato |
| N/A | Non Applicabile |

| | |
|----------|-------------------------------|
| 1 | Business Impact Analysis |
| 2 | Business Continuity Procedure |
| 3 | Comitato BC |
| 5 | Disaster Recovery Plan |

| | |
|----------|-----------------------------|
| 6 | Disaster Recovery Plan |
| 7 | Disaster Recovery Strategia |
| 8 | Comunicazione |
| 9 | Test di Disaster Recovery |

Copyright © 2022 – Nethive SPA

È vietata la riproduzione anche parziale di quanto pubblicato.
Il presente materiale è consegnato come base di partenza propria struttura e alle procedure della azienda.

Business Continu

Requisiti Richiesti

Requisiti generali dei fornitori

Le risorse (es: hardware, dispositivi, dati, allocazione temporale, personale e software) sono prioritizzate in base alla loro classificazione (e.g. confidenzialità, integrità, disponibilità), criticità e valore per il business dell'organizzazione. È stata svolta una Business Impact Analysis, la stessa è formalizzata e periodicamente aggiornata.

E' definita e implementata una politica di business continuity, con l'obiettivo di per garantire la continuità delle attività essenziali allo svolgimento del Business, a fronte di qualunque evento che ne renda indisponibili le strutture o i servizi (edifici, impianti, attrezzature, sistemi informativi, ecc.) per un periodo di tempo prolungato.

Sono definiti i ruoli delle figure con ruolo chiave durante un evento che impatta la Continuità Operativa

Esiste un piano di ripristino (recovery plan) e viene eseguito durante o dopo un incidente di cybersecurity.
I processi e le procedure di ripristino sono eseguite e mantenute per assicurare un recupero dei sistemi o asset coinvolti da un incidente di cybersecurity.

Il piano di DR è conosciuto dalle persone che devono metterlo in atto, e disponibile in qualsiasi momento anche distrattosi alle risorse che ne devono avere accesso

Sono organizzati e svolti periodici audit con l'obiettivo di monitorare la corretta esecuzione delle attività pianificate.
Gli audit sono documentanti.

Le attività di ripristino condotte a seguito di un incidente vengono comunicate alle parti interessate interne ed esterne all'organizzazione, inclusi i dirigenti ed i vertici dell'organizzazione

I processi e le procedure di ripristino sono periodicamente testate e mantenute al fine di verificare che il personale svolga adeguatamente quanto pianificato, e che le stesse procedure sia coerenti nel tempo.

ato senza la preventiva autorizzazione scritta di Nethive.
e per la costruzione di un proprio impianto o sistema di gestione. Si

ity e Disaster Recovery

| Campi per il Fornitore | |
|---|---|
| Valutazione stato di applicazione del requisito | Integrazione requisito ed evidenze a supporto |

| | |
|--|--|
| | |
| | |
| | |
| | |

| | |
|--|--|
| | |
| | |
| | |
| | |

| | |
|---|---------------------------------------|
| o | VALUTAZIONE IMPLEMENTAZIONE REQUISITI |
|---|---------------------------------------|

consiglia di adeguare i contenuti e alla

| LEGENDA STATO IMPLEMENTAZIONE | |
|-------------------------------|---------------------------------------|
| 0 | Non ancora implementato/pianificato |
| 1 | Parzialmente implementato/Pianificato |
| 2 | Completamente implementato |
| N/A | Non Applicabile |